

Délibération n° 2018-011 du 17 janvier 2018

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion et supervision de la messagerie électronique professionnelle utilisée à des fins de surveillance et de contrôle* »

présenté par la Société Générale (Monaco)

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financier ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée ;

Vu la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Arrêté Ministériel n° 2012.199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la délibération n° 2015-111 du 18 novembre 2015 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle* » ;

Vu la délibération n° 2017-156 du 20 septembre 2017 de la Commission de Contrôle des Informations Nominatives portant autorisation de transfert d'informations nominatives ayant pour finalité « *Transfert d'informations nominatives à la Société Générale Global Solution Centre Pvt. Ltd (SGGSC) en Inde aux fins de maintenance informatique et assistance technique* » ;

Vu la demande d'autorisation déposée par la Société Générale (Monaco) le 16 octobre 2017 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique professionnelle utilisée à des fins de surveillance et de contrôle* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 décembre 2017, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 janvier 2018 portant examen du traitement automatisé susvisé.

## **La Commission de Contrôle des Informations Nominatives,**

### **Préambule**

La Société Générale (Monaco) est la succursale à Monaco de la Société Générale SA, établissement bancaire français (Paris), immatriculé au répertoire du Commerce et de l'Industrie sous le numéro 62S01045, qui a pour activité « *Opérations de banque* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de cette société disposent d'une messagerie professionnelle faisant l'objet d'une supervision.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance. Il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

### **I. Sur la finalité et les fonctionnalités du traitement**

Ce traitement a pour finalité « *Gestion et supervision de la messagerie électronique professionnelle utilisée à des fins de surveillance et de contrôle* ».

Les personnes concernées sont les employés, les clients et les tiers externes.

Enfin, le responsable de traitement indique que les fonctionnalités sont les suivantes :

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'historisation des messages électroniques entrants ou sortants ;
- la gestion des contacts de la messagerie électronique ;
- la gestion des dossiers de la messagerie et des messages archivés ;
- l'établissement et la lecture de fichiers journaux ;

- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda ;
- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques entrants et sortants ;
- l'établissement de preuves en cas de litige avec un client/employé.

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

## **II. Sur la licéité et la justification du traitement**

### **➤ Sur la licéité**

Dans le cadre de sa recommandation n° 2015-111 du 18 novembre 2015, la Commission rappelle les conditions de licéité d'un traitement de messagerie professionnelle, au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Elle relève notamment que l'article 34 de l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 dispose que « *le responsable du contrôle permanent s'assure de [...] l'application de procédures garantissant la prise en compte conforme des instructions de la clientèle et des opérations diverses sur instruments financiers [...]* ».

Par ailleurs, l'article 4 de la Loi n° 1.362 du 3 août 2009 dispose que les organismes bancaires « *doivent exercer une vigilance constante à l'égard de la relation d'affaires en examinant les transactions [...] conclues pendant toute sa durée [...]* ».

La Commission considère donc que le traitement est licite au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

### **➤ Sur la justification**

Le responsable de traitement indique que le traitement est justifié par « *le respect d'une obligation légale à laquelle est soumis le responsable de traitement ou son représentant* », et par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission observe que ce traitement permet au responsable de traitement de respecter notamment les obligations découlant des Lois n° 1.314 du 29 juin 2006, n° 1.338 du 7 septembre 2007 et n° 1.362 du 3 août 2009.

Par ailleurs, le responsable de traitement indique que ce traitement répond à un objectif légitime essentiel puisqu'il permet :

- l'optimisation de l'accomplissement des missions de travail des employés de l'entité par l'accroissement de la qualité du traitement des opérations qui permet d'améliorer la gestion de la relation Banque/client ;
- la sécurité et le bon fonctionnement technique du système d'information ;
- le contrôle du respect des instructions internes, des règles de sécurité et des recommandations de l'audit relatives à l'utilisation de la messagerie professionnelle, facilitant ainsi l'instruction des dossiers de fraude ;
- la préservation des intérêts économiques, commerciaux et financiers de la banque à travers la sécurité des échanges d'informations financières et/ou économiques relatives aux projets ou à la conception, la fabrication, la production, les caractéristiques et tarifications des

- services et produits proposés par l'entité,...et plus généralement à la sécurité de ses activités ;
- la protection contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice, par la préservation de la confidentialité des données et des informations auxquelles l'entité et le personnel accèdent dans le cadre de leurs activités et qui peuvent être échangées à travers les messageries électroniques ;
  - le contrôle de la régularité et de la conformité de certaines opérations qui pourraient être adressées et/ou traitées par messagerie.

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque « *le traitement ne fait l'objet d'aucune surveillance nominative permanente* » et que les contrôles sont mensuels, « *aléatoires et réalisés sur 5 boîtes mails au maximum* ».

Il indique par ailleurs que les messages privés sont exclus du domaine des contrôles et que sont considérés comme privés les messages « *comportant, à l'émission ou à la réception, le mot clé « [PRV] » (sans tenir compte des accents ou des minuscules/majuscules), dans le champ objet* ».

A cet égard, la Commission rappelle, conformément à de sa délibération n° 2015-111 du 18 novembre 2015, que « *seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi* ».

Elle constate enfin que conformément à sa délibération n° 2015-111 du 18 novembre 2015, des dispositions ont été prises afin d'assurer la continuité des affaires de la société en cas d'absence ou de départ d'un employé.

Aussi la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

### **III. Sur les informations nominatives traitées**

Les informations nominatives traitées sont :

- identité : nom, prénom, identifiant ;
- données d'identification électronique : adresse de messagerie électronique, adresse générique ;
- messages : contenu de la messagerie et des messages, objets, dossiers de classement et d'archivage en ligne, pièces jointes et fichiers créés dans la messagerie (hors archives locales/ hors messages privés) ;
- gestion des contacts : nom prénom, raison sociale, (...)
- informations temporelles : date et heure de réception/envoi de messages ;
- log d'accès : identifiants de connexion, logs de connexion des personnes habilitées à avoir accès au traitement, y compris les utilisateurs de la messagerie ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format et nature des pièces jointes, noms de domaine expéditeurs de messages ;
- gestion des alertes : réception des alertes automatiques en fonction des niveaux hiérarchiques concernés ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, types de droits conférés, historisation des habilitations.

Le responsable de traitement indique que les informations relatives à l'identité, aux données d'identification électroniques, aux messages, à la gestion des contacts et aux informations temporelles ont pour origine le compte de messagerie.

Les informations relatives aux logs d'accès, aux fichiers journaux, à la gestion des alertes et aux habilitations sont générées par le système informatique.

Aussi, la Commission considère que les informations traitées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

#### **IV. Sur les droits des personnes concernées**

##### **➤ *Sur l'information préalable des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée pour les clients par le biais des Conditions Générales d'utilisation, pour les employés par le biais d'une note de service et d'une charte d'utilisation des moyens de communication électronique et enfin pour les tiers extérieurs par le biais d'une mention insérée au bas de tout message électronique sortant.

A l'analyse de ces documents, la Commission considère que les modalités d'information préalable des personnes sont conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

##### **➤ *Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès s'exerce par voie postale auprès du Service Conformité pour les clients et les tiers, et auprès du Service Ressources Humaines pour les employés.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

Sous cette condition, elle considère que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

#### **V. Sur les personnes ayant accès au traitement et les destinataires**

##### **➤ *Sur les personnes ayant accès au traitement***

Le responsable de traitement indique que les personnes ayant accès au traitement sont :

- les supérieurs hiérarchiques des personnes concernées par le traitement : en consultation ;
- les services Déontologie, Juridique et Contentieux : en consultation ;
- les agents habilités par le propriétaire de la messagerie lui-même : en consultation ;
- les administrateurs système du Service Informatique : tous accès dans le strict cadre de l'accomplissement de leurs missions techniques et de maintenance système ;
- l'équipe SAFE (Security & AntiFraude Expertise, filière interne de la Société Générale) à Bucarest : traitement des alertes DLP ;
- les équipes support/ maintenance habilités du Centre de Service partagé interne à la Société Générale basé en Inde : en inscription, modification, mise à jour et consultation.

Concernant cette dernière catégorie, la Commission note que les accès distants par les équipes situées en Inde ont été autorisés par la Commission par sa délibération n°2017-156 du 20 septembre 2017, à des fins de maintenance informatique et d'assistance technique.

Ladite autorisation de transfert ne concernait que les catégories d'informations suivantes : identité, situation de famille, données d'identification électronique et données relatives à l'emploi occupé.

En conséquence, si d'autres informations nominatives, dont notamment les contenus des messages échangés, devaient être rendues accessibles depuis l'Inde, elle rappelle qu'une demande d'autorisation de transfert modificative devra lui être soumise préalablement à la mise en place de ces accès.

Sous réserve de ce qui précède, la Commission considère que les accès susvisés sont justifiés.

Elle prend acte en outre des précisions du responsable de traitement selon lesquelles « aucune de ces personnes ne pourra avoir accès aux contenus des messages électroniques identifiés comme privés ».

La Commission considère toutefois que les utilisateurs de la messagerie ont également accès au traitement en émission, réception, consultation et suppression pour les messages émis et reçus par eux.

Elle constate enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, la liste nominative des personnes ayant accès au traitement est tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

#### ➤ **Sur les communications d'informations**

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Elle considère donc que de telles transmissions sont conformes aux exigences légales.

## **VI. Sur les rapprochements et interconnexions avec d'autres traitements**

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion et traçabilité des habilitations informatiques* » qui a été légalement mis en œuvre.

## **VII. Sur la sécurité du traitement et des informations**

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

La Commission relève néanmoins que l'architecture technique repose sur des équipements de raccordement (switchs, routeurs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

Elle rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2015-111 du 18 novembre 2015.

La Commission rappelle également que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

## **VIII. Sur la durée de conservation**

Le responsable de traitement indique que les informations relatives à l'identité, aux données d'identification électronique et à la gestion des contacts sont conservées 3 mois maximum après le départ de l'utilisateur.

Par ailleurs, les informations temporelles, les logs d'accès, les fichiers journaux, les informations relatives à la gestion des alertes et les habilitations sont conservées 1 an maximum.

Enfin, conformément à la délibération n° 2015-111 du 18 novembre 2015 une politique d'archivage est mise en place pour le contenu des messages émis et reçus jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

La Commission considère donc que ces durées sont conformes aux exigences légales.

### **Après en avoir délibéré, la Commission :**

**Considère que** les utilisateurs de la messagerie ont également accès au traitement en émission, réception, consultation et suppression pour les messages émis et reçus par eux.

**Constata que** la liste nominative des personnes ayant accès au traitement est tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

### **Rappelle :**

- qu'une demande d'autorisation de transfert modificative devra lui être soumise si d'autres informations nominatives que celles autorisées par sa délibération n° 2017-156 devaient être accessibles depuis l'Inde ;
- que le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- que les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;
- que les équipements de raccordement (switchs, routeurs, pare-feux) de serveurs et périphériques doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés ;
- que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

**A la condition de la prise en compte de ce qui précède,**

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Société générale (Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique professionnelle utilisée à des fins de surveillance et de contrôle* ».**

Le Président

Guy MAGNAN